



FIG. 1  
(PRIOR ART)

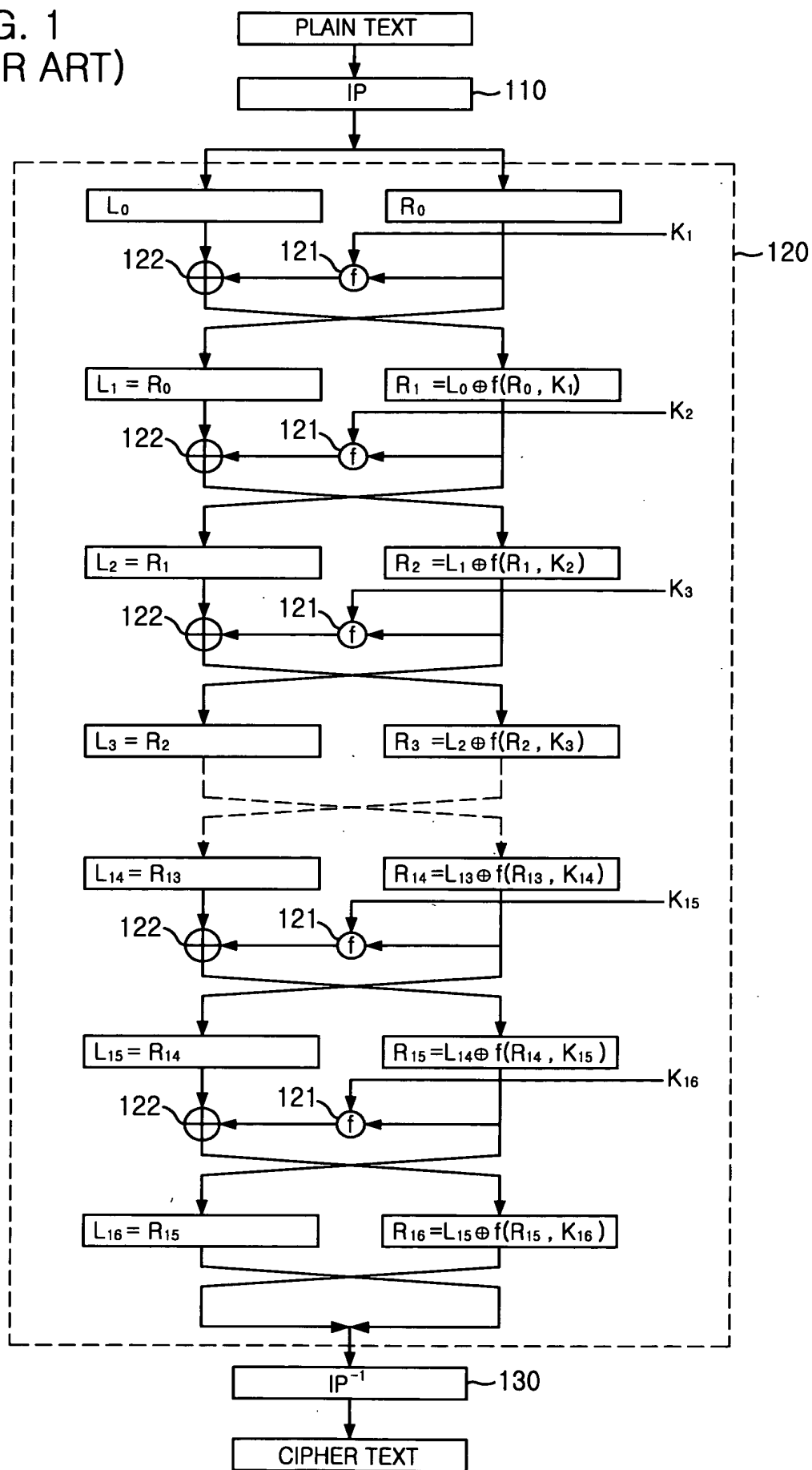


FIG. 2  
(PRIOR ART)

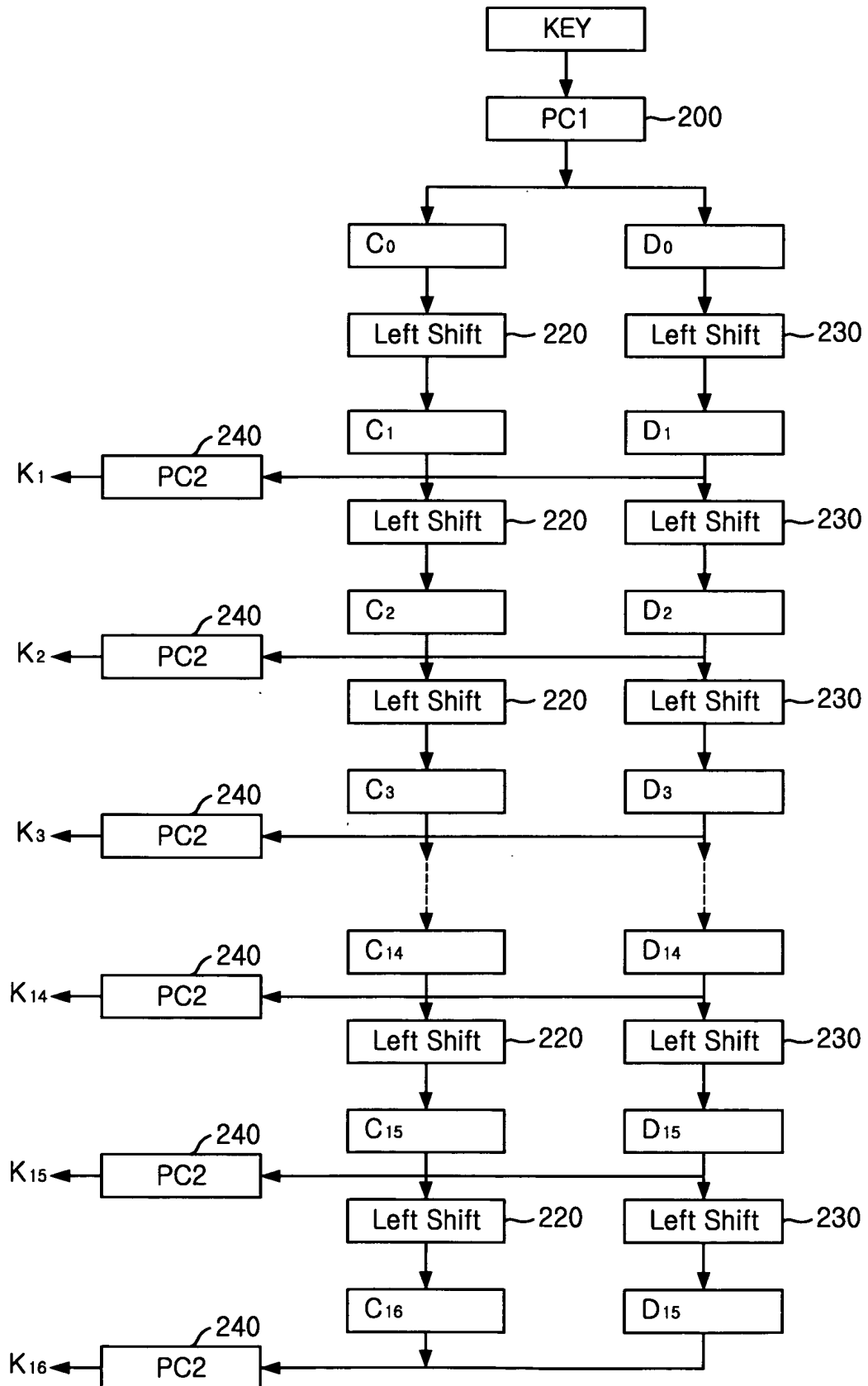


FIG. 3  
(PRIOR ART)

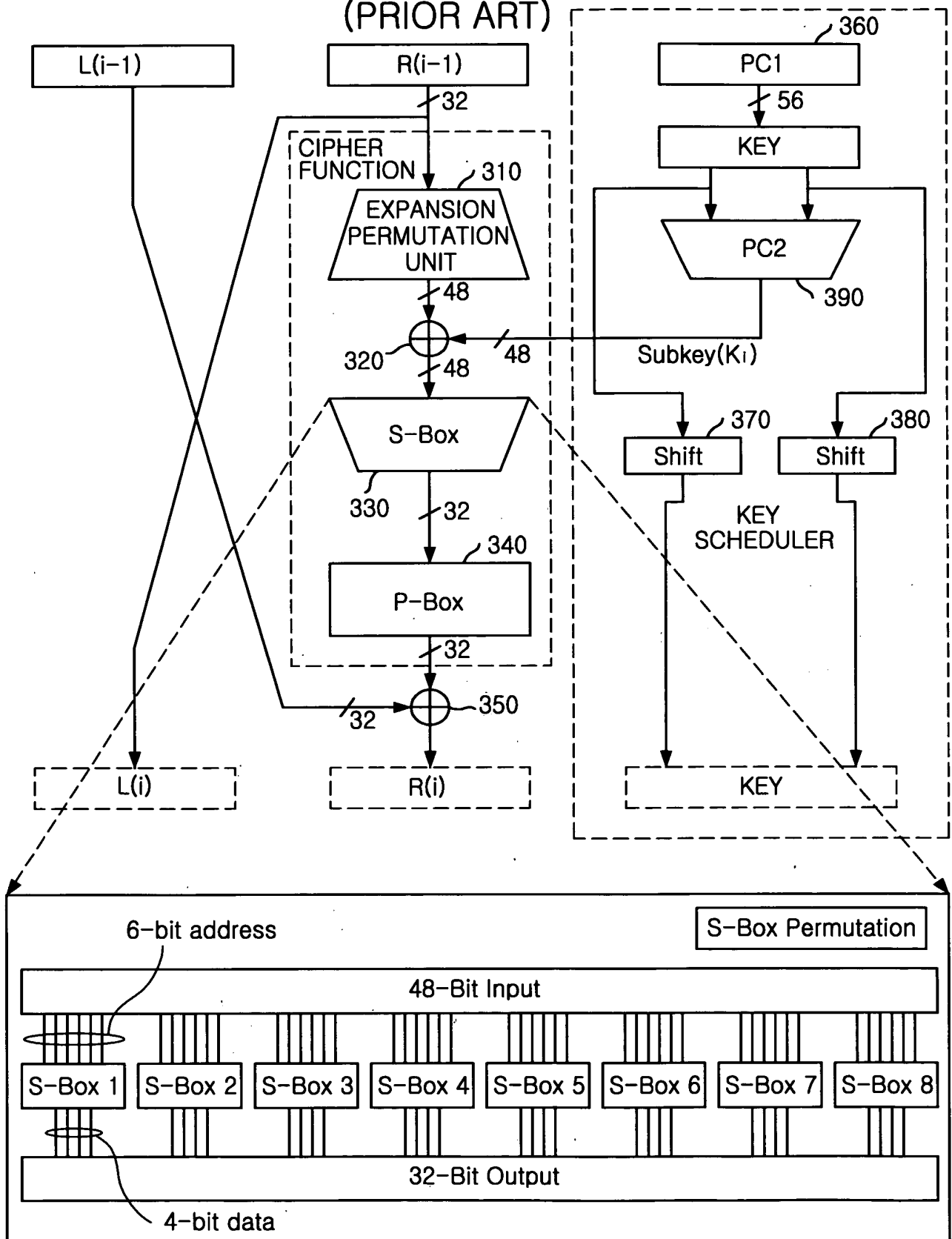


FIG. 4  
(PRIOR ART)

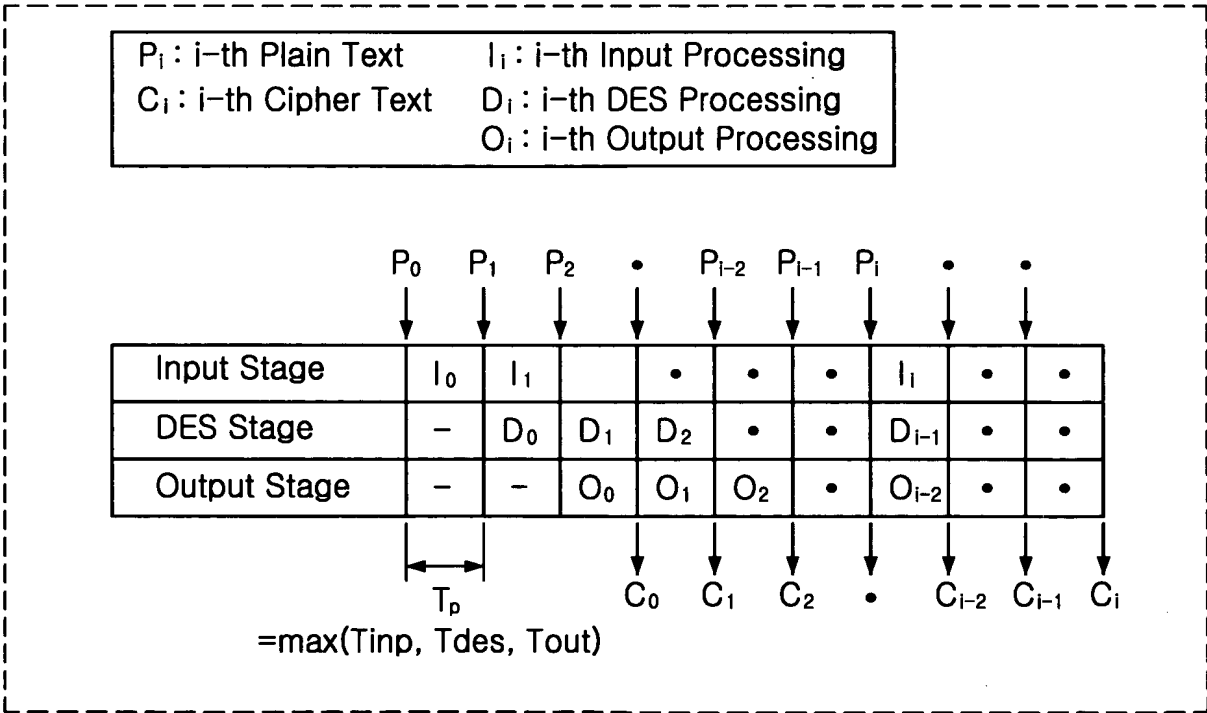
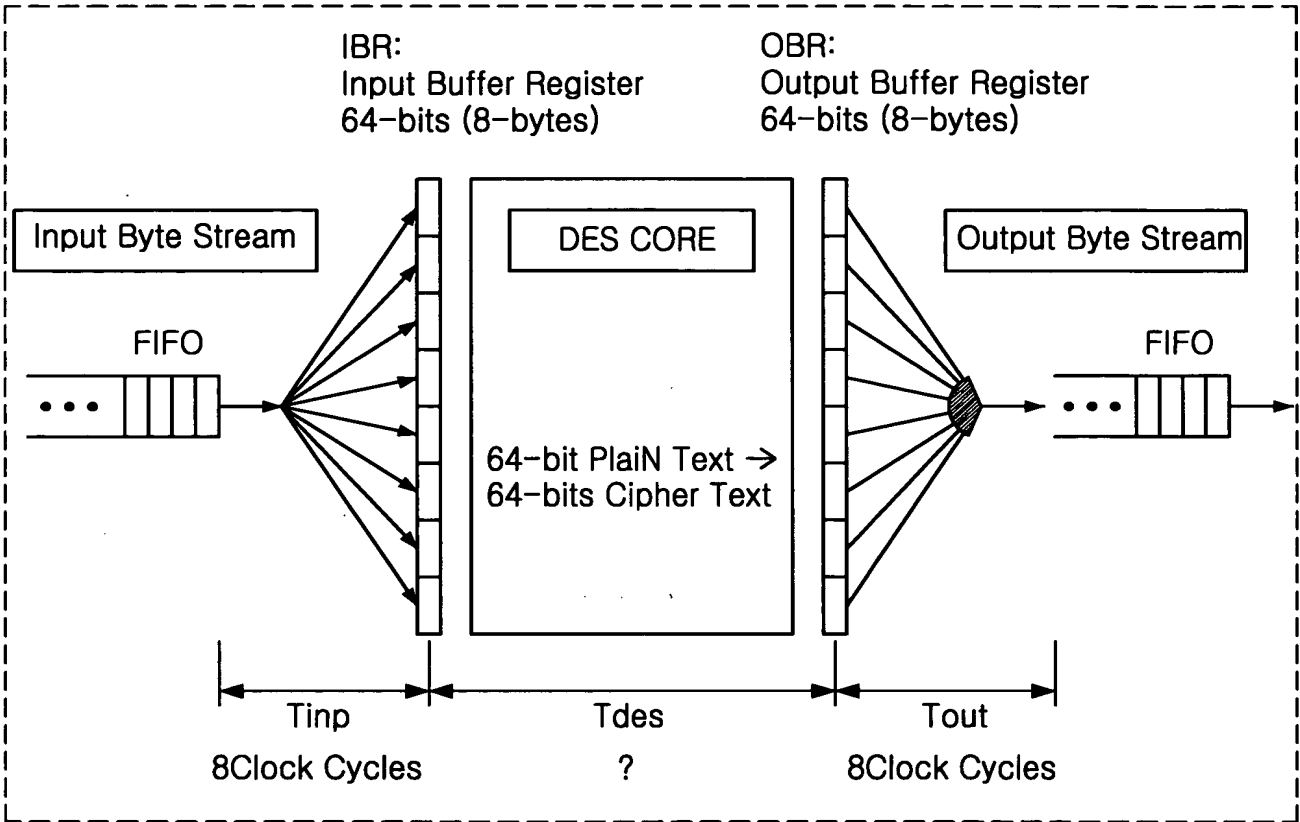


FIG. 5A  
(PRIOR ART)

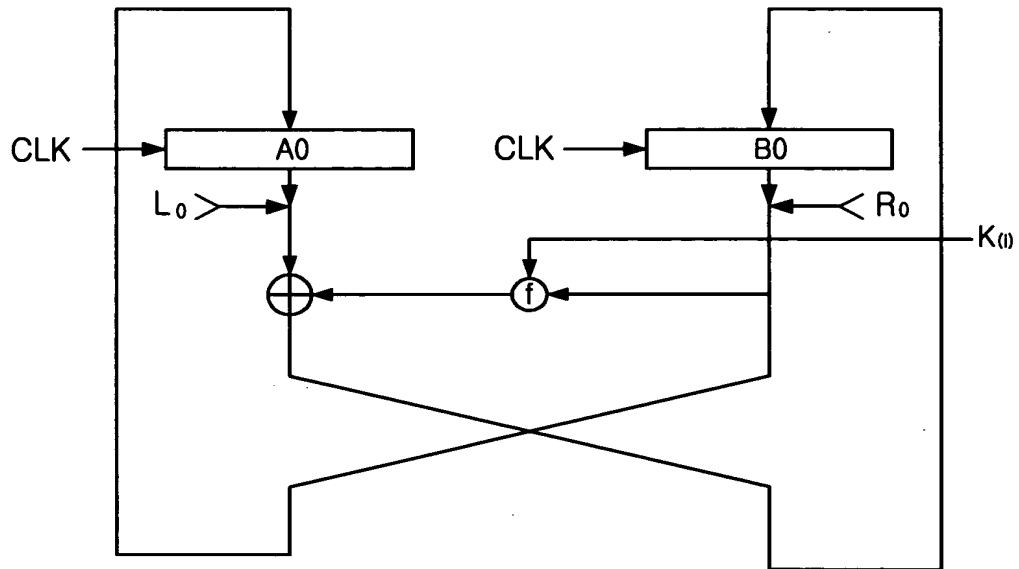


FIG. 5B

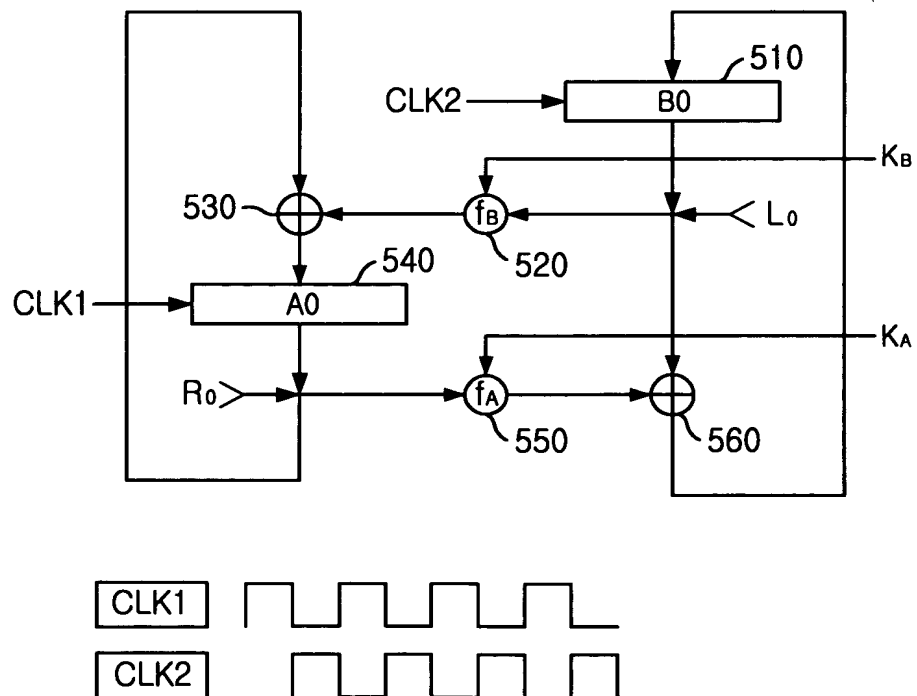


FIG. 6

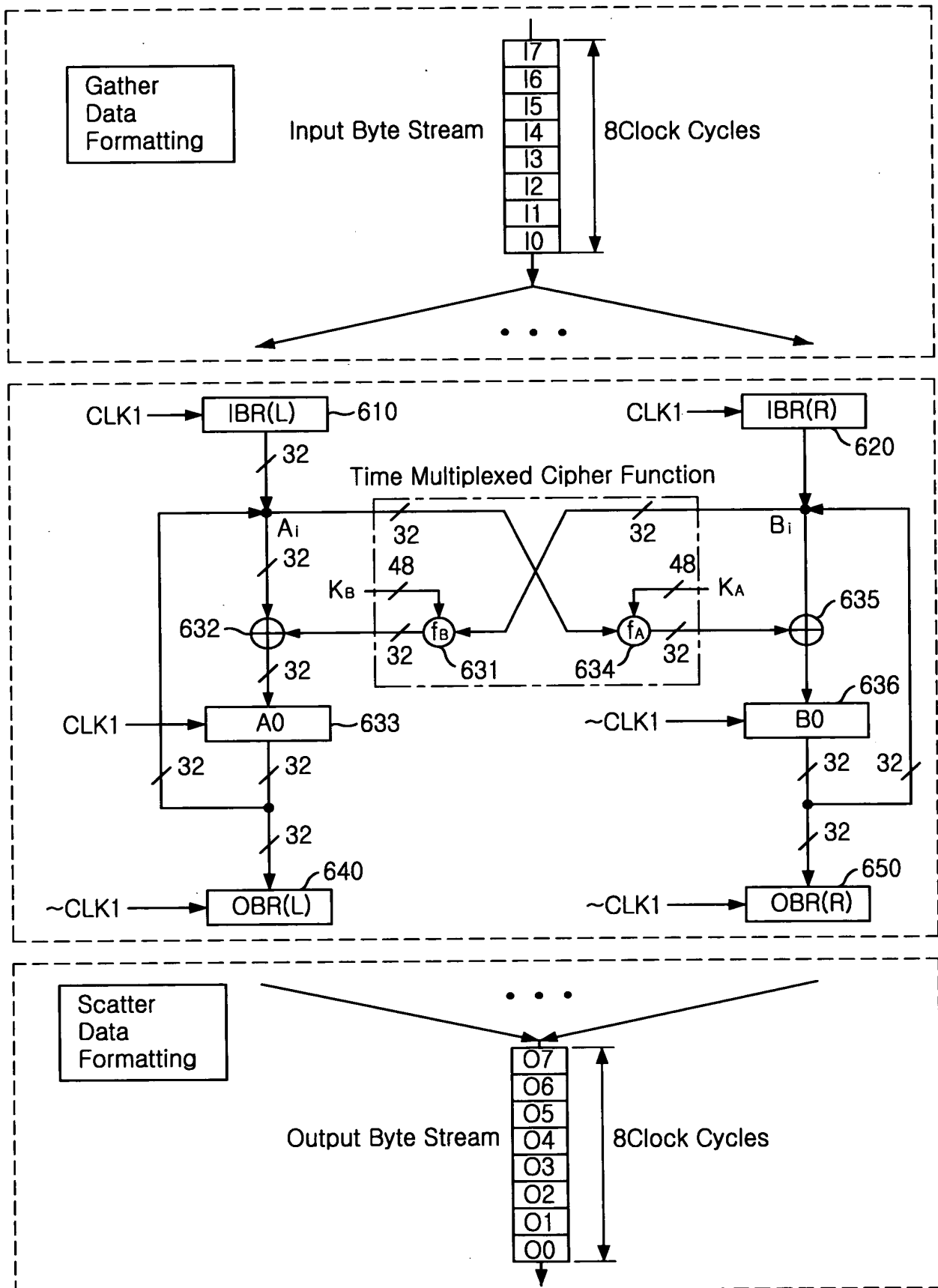


FIG. 7

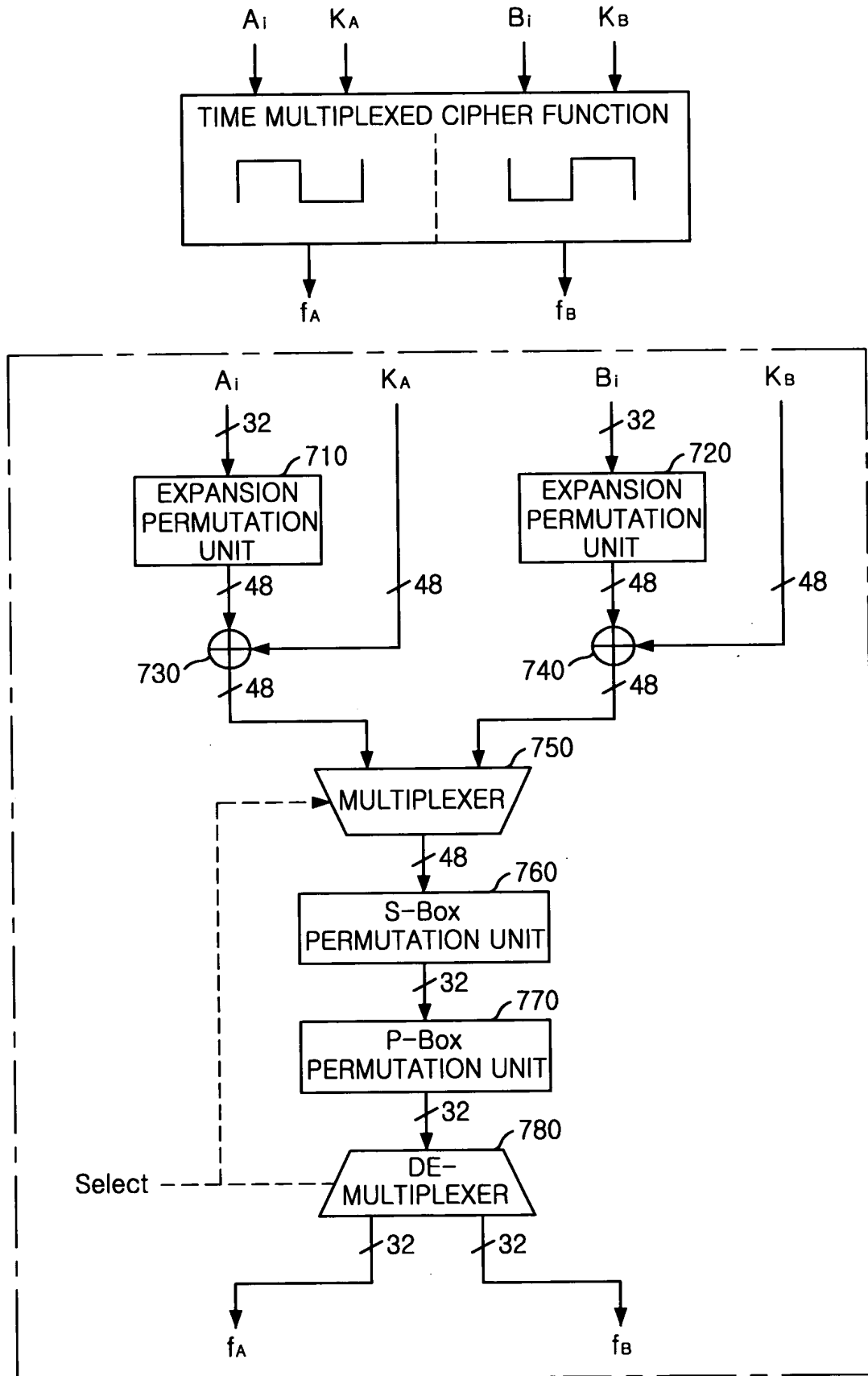
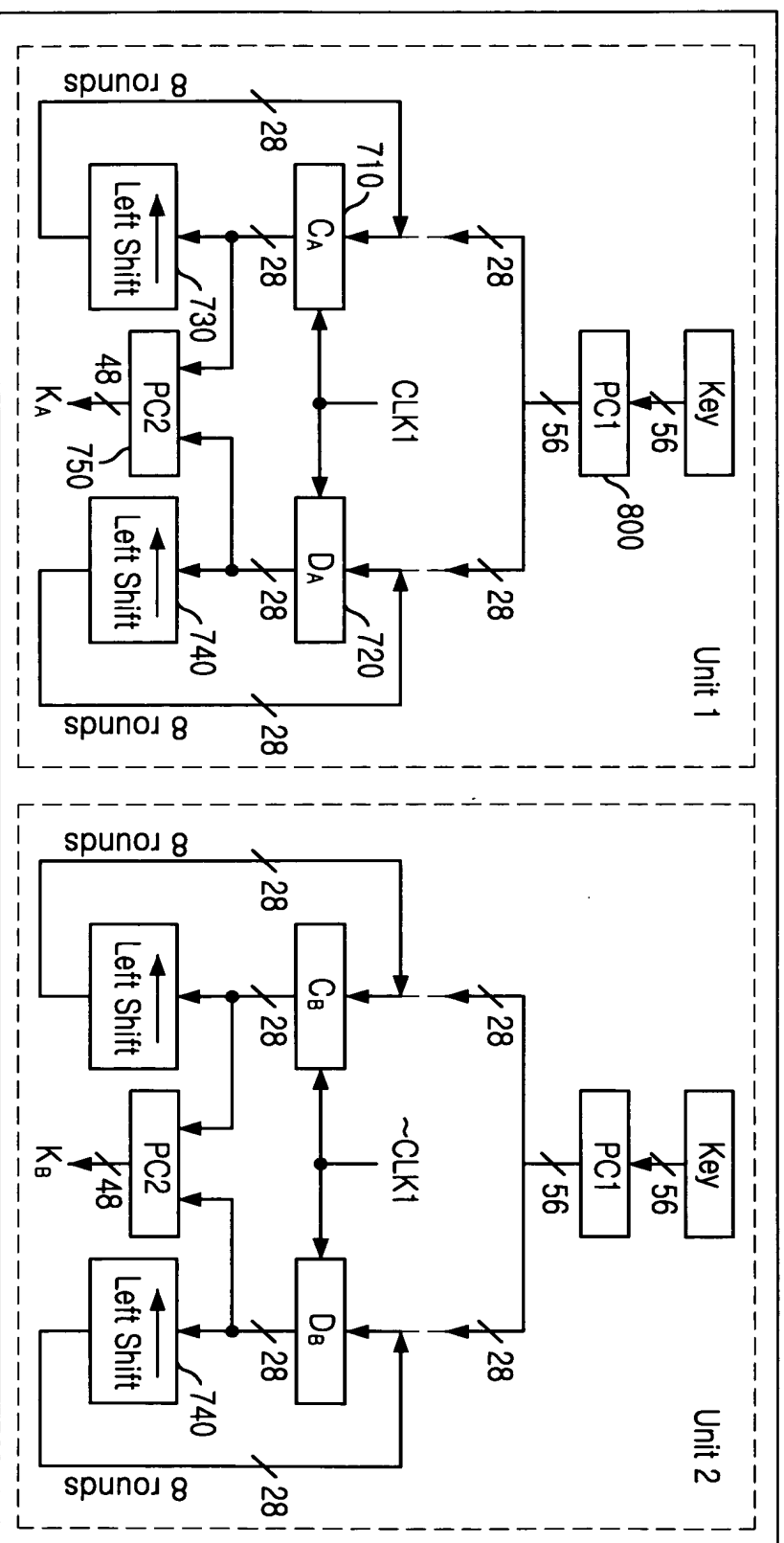


Fig. 8

Round	Left Shift Amount	Total Shift Amount
1( $P_0$ )	3	1
2( $P_1$ )	4	4
3( $P_2$ )	4	8
4( $P_3$ )	3	12
5( $P_4$ )	4	15
6( $P_5$ )	4	19
7( $P_6$ )	4	23
8( $P_7$ )	2	27

Round	Left Shift Amount	Total Shift Amount
1(Q <sub>0</sub> )	4	2
2(Q <sub>1</sub> )	4	6
3(Q <sub>2</sub> )	4	10
4(Q <sub>3</sub> )	3	14
5(Q <sub>4</sub> )	4	17
6(Q <sub>5</sub> )	4	21
7(Q <sub>6</sub> )	3	25
8(Q <sub>7</sub> )	2	0

WHEN KEY IS LOADED FIRST TIME, IT SHOULD BE 1





# FIG. 9

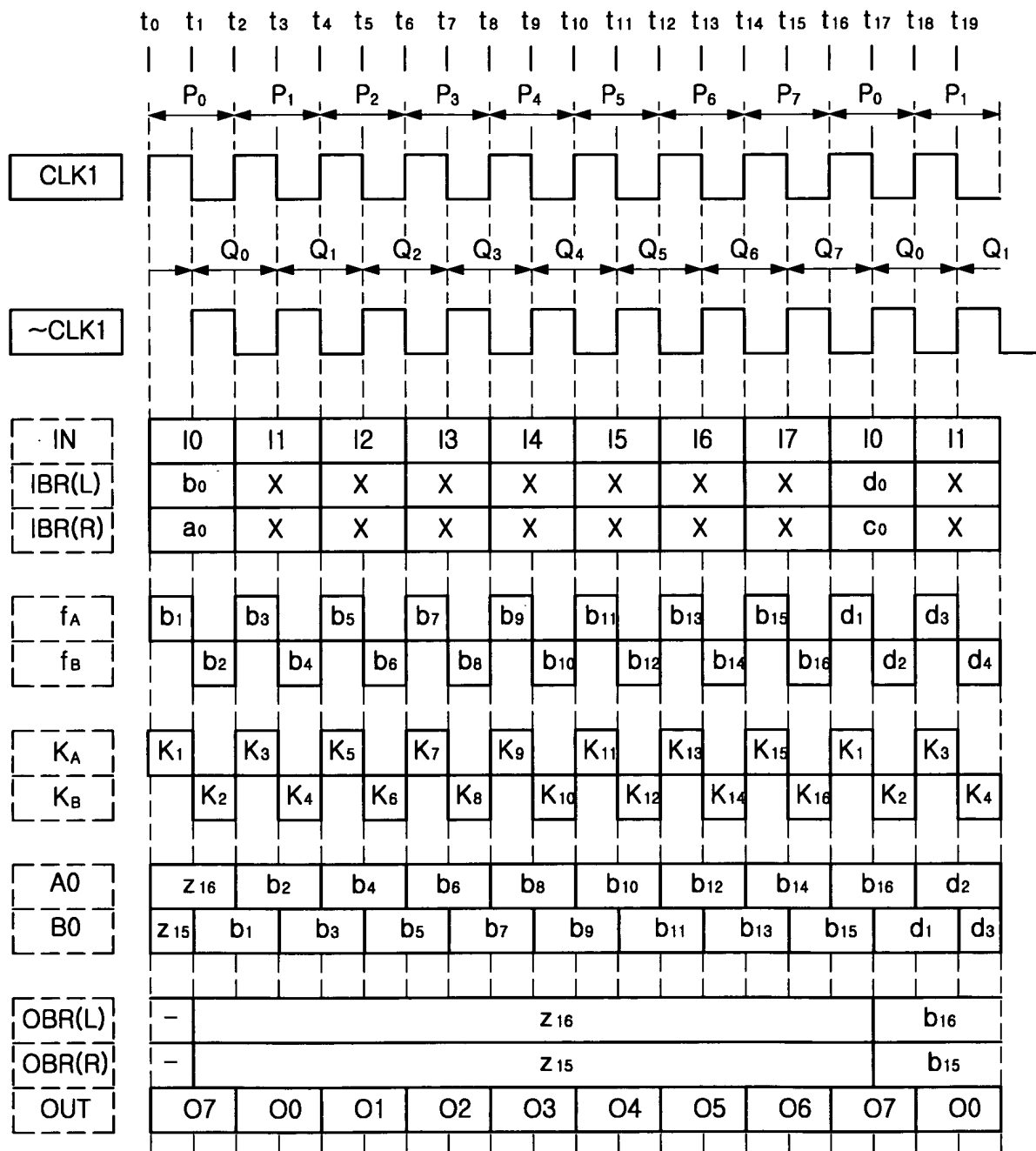


FIG. 10

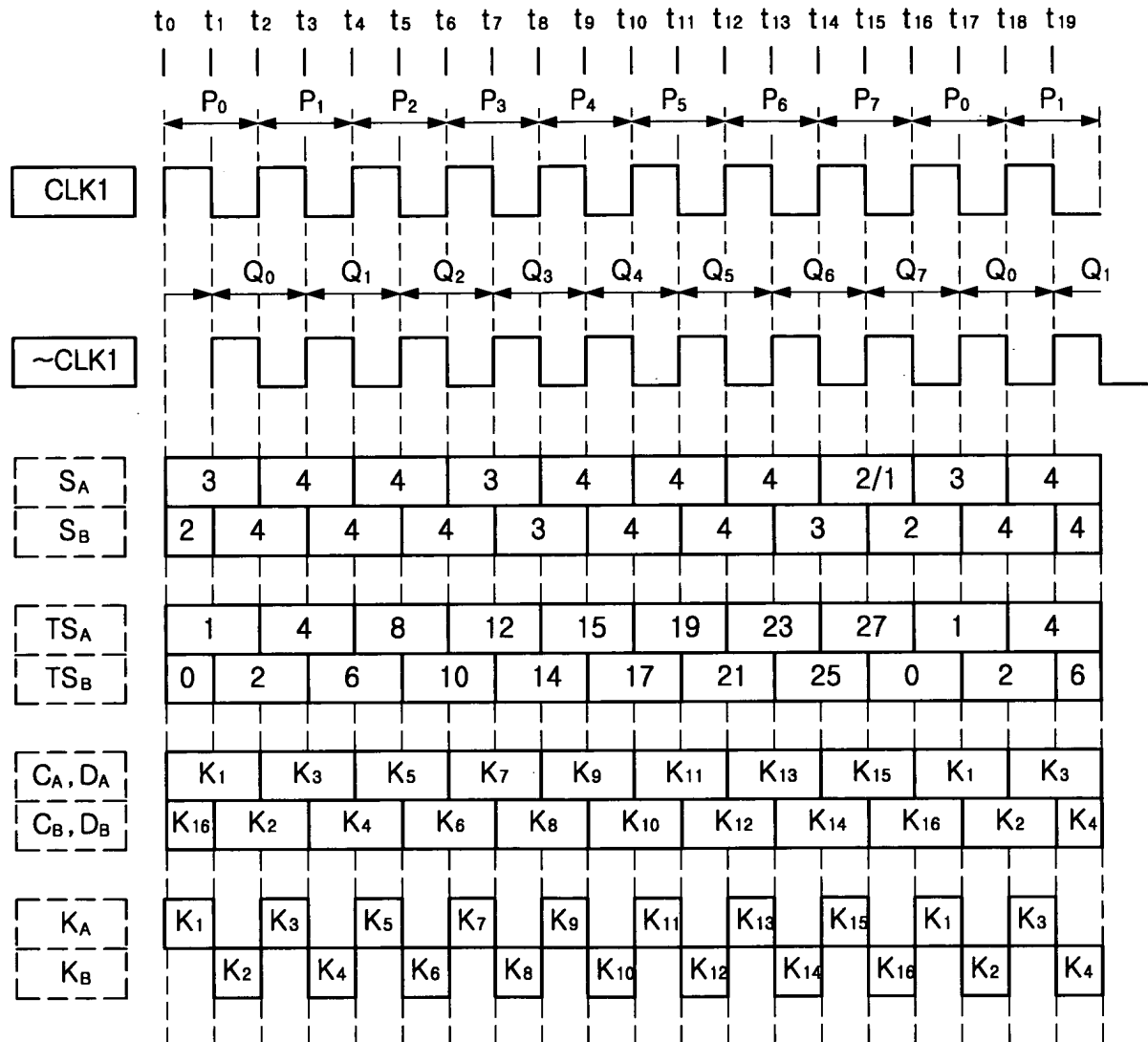


FIG. 11

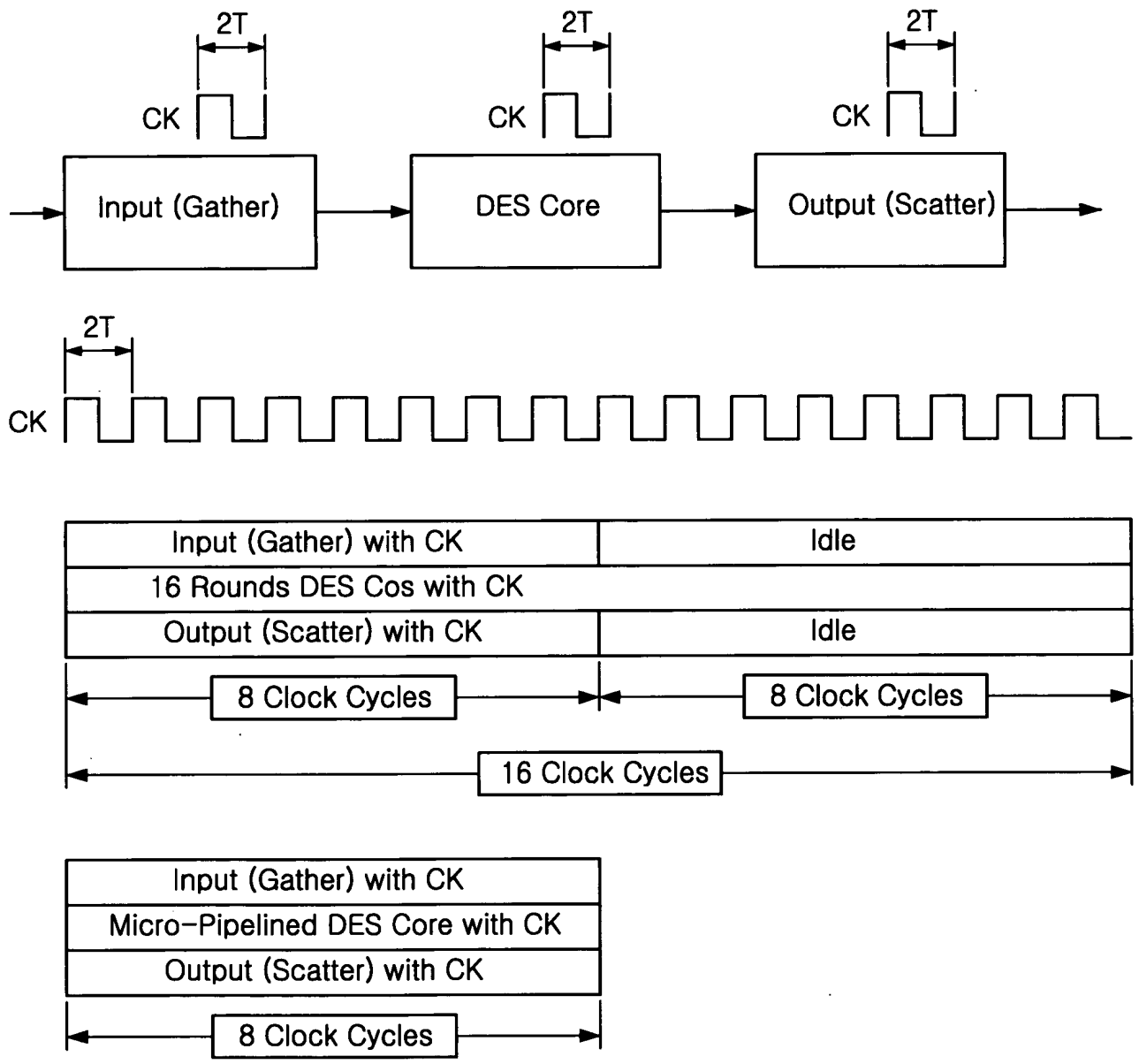


FIG. 12

